Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
Telephone: 725-235-9750
Email: LasVegas@StranchLaw.com

[*Additional counsel on signature page*]

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

KAREN SMITH, PHOLISITH BOUPHAPRASEUTH, RYAN FARRELL, SUSAN STEVENS, and JAY SAX, individually and on behalf of all others similarly situated, Plaintiffs, v. FINDLAY AUTOMOTIVE, INC., Defendant.	Case No. 2:24-cv-01226-RFB-EJY **CONSOLIDATED CLASS COMPLAINT**

Plaintiffs Karen Smith, Pholisith Bouphapraseuth, Ryan Farrell, Susan Stevens, and Jay Sax ("Plaintiffs"), individually, and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant Findlay Automotive, Inc. ("Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations on information and belief, except as to their own actions, which are made on personal knowledge, the investigation of counsel, and the facts that are a matter of public record.

INTRODUCTION

1. This class action arises out of the recent targeted ransomware attack and data breach ("Data Breach") on Defendant's network that resulted in unauthorized access and acquisition of Plaintiffs' highly sensitive data. As a result of the Data Breach, Class Members suffered

ascertainable losses in the form of the failure to receive agreed-upon compensation, benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the present risk of imminent harm caused by the compromise of their sensitive personal information, including their financial information and social security numbers.

2. Upon information and belief, the specific information compromised in the Data Breach includes, but is not limited to, personally identifiable information ("PII"), such as full names, addresses, driver's license numbers, and social security numbers, insurance policy numbers, credit and debit card numbers, and financial and credit-related information.[1]

3. Upon information and belief, up to and through June 2024, Defendant obtained the PII of Plaintiffs and Class Members and stored that PII, unencrypted, in an Internet-accessible environment on Defendant's network, from which unauthorized actors used an extraction tool to retrieve sensitive PII belonging to Plaintiffs and Class Members.

4. Plaintiffs' and Class Members' PII—which were entrusted to Defendant, their officials, and agents—were compromised and unlawfully accessed due to the Data Breach.

5. Defendant was also not prepared to respond to a Data Breach and has seen significant disruption to its business operations.

6. Defendant's lack of preparedness furthermore prevented customers from being paid money Defendant owed them. Rather than pay those customers, Defendant merely told them that the payments were delayed due to the cyberattack.

7. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of his and Class Members' PII that Defendant collected and maintained, and to seek reimbursement for the harm caused by Defendant's failure to timely pay monies they owe to Class Members.

8. Defendant maintained the PII in a negligent and/or reckless manner. In particular,

[1] *See* https://www.findlayauto.com/privacy-policy-and-cookie-policy/ (describing categories of PII collected by Defendant).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

9. In addition, upon information and belief, Defendant and its employees failed to properly monitor the computer network, IT systems, and integrated services that housed Plaintiffs' and Class Members' PII, including either through the lack of sufficient centralized monitoring and alerting systems or through the use of third-party managed services providers, such Defendant failed to timely recognize malicious activity on its information systems.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of malicious cybercriminals. The risks to Plaintiffs and Class Members will remain for their respective lifetimes.

11. Moreover, Defendant's failures have materially affected Plaintiffs' and Class Members' financial stability because it has delayed Defendant's ability to process payments to Plaintiffs' and Class Members.

12. Defendant failed to provide timely, accurate, and adequate notice to Plaintiffs and Class Members. Plaintiffs' and Class Members' knowledge about the PII Defendant lost, as well as precisely what type of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Defendant's failure to warn impacted persons immediately upon learning of the Data Breach.

13. Indeed, armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to target other phishing and hacking intrusions using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members'

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a present, heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now closely monitor their financial accounts to guard against identity theft for the rest of their lives.

15. Plaintiffs and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Moreover, Plaintiffs and Class Members have been deprived of the use of their financial resources because of Defendant's failure to properly Defendant against cyberattacks or to properly have a plan in place for how to handle funds processing in the event of such an attack.

17. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals who have suffered harm due to Defendant's failures.

18. Accordingly, Plaintiffs bring claims on behalf of themselves and the Class for: (i) negligence, (ii) breach of contract, (iii) invasion of privacy, (iv) unjust enrichment, and (iv) declaratory judgment and injunctive relief. Through these claims, Plaintiffs seek, *inter alia*, damages and injunctive relief, including improvements to Defendant's data security systems and integrated services, future annual audits, and adequate credit monitoring services.

PARTIES

19. Plaintiff Farrell is a natural person and citizen of Nevada.

20. Plaintiff Smith is a natural person and citizen of Nevada.

21. Plaintiff Bouphapraseuth is a natural person and citizen of Nevada.

22. Plaintiff Graham Pyle is a natural person and citizen of Nevada.

23. Plaintiff Susan Stevens is a natural person and citizen of Nevada.

24. Defendant is a Nevada corporation with its principal place of business located in Henderson, Clark County, Nevada.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

JURISDICTION AND VENUE

25. The Court has subject matter jurisdiction over this matter pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5,000,000, exclusive of interests and costs. The number of proposed class members is well over 100, and some of those class members reside outside of the State of Nevada given that Defendant owns dealerships in multiple states.

26. The Court has personal jurisdiction over Defendant in that it operates in this State and District.

27. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's headquarters in this District and a substantial portion of the events giving rise to these claims occurred in this District.

BACKGROUND FACTS

A. Defendant's Business

28. Established in 1961 in Las Vegas, Nevada, Defendant operates 35 automobile dealerships located in Nevada, Arizona, Utah, Idaho, and Washington and sells dozens of automobile brands.[2]

29. On information and belief, Defendant maintains the PII of consumers to whom it sells and leases vehicles, including but not limited to their full names, addresses, driver's license numbers, and social security numbers, insurance policy numbers, credit and debit card numbers, and financial and credit-related information, and other information that Defendant may deem necessary to provide its services.

30. In addition to selling automobiles, Defendant also purchases automobiles from its customers, like Plaintiffs, including on a trade-in basis.

31. Plaintiffs and Class Members directly or indirectly entrusted Defendant with

[2] *See* Sean Hemmersmeier, *Cybersecurity Attack Impacts Sales, Service at Nevada Automotive Group* (June 10, 2024, 5:47 PM), https://www.reviewjournal.com/business/cybersecurity-attack-impacts-sales-service-at-nevada-automotive-group-3066257; *see also* https://www.findlayauto.com.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial crimes.

32. Because of the highly sensitive and personal nature of the information Defendant acquires, stores, and has access to, Defendant, upon information and belief, promised to, among other things: keep PII private; comply with industry standards related to data security and PII; inform individuals of their legal duties and comply with all federal and state laws protecting PII; only use and release PII for reasons that relate to medical care and treatment; and provide adequate notice to impacted individuals if their PII is disclosed without authorization.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

34. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

35. Plaintiffs and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

36. Defendant recognizes that it owes duties to protect Plaintiffs' and Class Members' PII. For example, in its "Privacy Policy," Defendant promises: "We implement reasonable security measures to ensure the security of your personal information."[3]

B. Defendant Fails to Safeguard Consumer PII.

37. Upon information and belief, Defendant's employees received "ransom notes" from a ransomware attacker after logging into their computers on June 9, 2024.

38. On or about June 10, 2024, Defendant announced it had been affected by a "cybersecurity issue" and issued the following statement on Facebook:

Findlay Automotive Group, which operates in Nevada, Utah, Arizona, Washington

[3] https://www.findlayauto.com/privacy-policy-and-cookie-policy.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

> and Idaho, recently identified a cybersecurity issue affecting certain areas of its IT systems. Promptly after becoming aware of the issue, we launched an investigation with the assistance of leading cybersecurity experts and law enforcement. Our investigation is ongoing, and we are working diligently to resolve the matter.
>
> All our locations are still open, although our ability to conduct sales and service is restricted. If you have a car in service at any Findlay Automotive dealership, we encourage you to personally stop by or telephone the service department to have our staff assist you.
>
> Findlay Automotive Group has been operating since 1961, and we take very seriously our responsibility to our customers and the community. We will continue to provide updates as the investigation continues and more information becomes available.[4]

39. Defendant has yet to directly notify Plaintiffs and Class Members that their PII has been compromised, or any other details of the Data Breach.

40. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) the PII of Plaintiffs and the Class Members.

41. Plaintiffs further believe their PII was likely subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals and now occurs in virtually every Data Breach, including in ransomware attacks because malicious actors exfiltrate the sensitive data contained on its target's systems before encrypting those same systems.

42. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

43. Because of the Data Breach, data thieves were able to gain access to Defendant's private systems and were able to compromise, access, and acquire the protected PII of Plaintiffs and Class Members.

44. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

45. Plaintiffs and the Class Members reasonably relied (directly or indirectly) on Defendant's sophistication to keep their sensitive PII confidential; to maintain proper system

[4] Samiksha Jain, *Findlay Automotive hit by Cybersecurity Attack, Investigation Ongoing* (June 12, 2024), https://thecyberexpress.com/findlay-automotive-cybersecurity-issue.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

46. Plaintiffs' and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The risks to Plaintiffs and Class Members will remain for their respective lifetimes.

47. Worryingly, the cybercriminals that obtained Plaintiffs' and Class Members' PII appear to be the notorious cybercriminal group "Scattered Spider."[5]

48. Scattered Spider is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about Scattered Spider. Specifically, the "Cybersecurity Advisory" states, *inter alia*, that: "Scattered Spider is a cybercriminal group that targets large companies and their contracted information technology (IT) help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual [tactics, techniques, and procedures]."[6]

49. Scattered Spider's ransomware strategy focuses on denial of service and extortion for stolen data. By encrypting systems and blocking access, they shut down operations from the inside, making it hard to do business. Ultimately, they exfiltrate the data and demand payment or threaten to release or use the data against its victims.[7]

C. Defendant was on Notice of the Foreseeable Risk of the Data Breach.

50. In light of recent high profile data breaches, Defendant knew or should have known,

[5] *See* https://x.com/LasVegasLocally/status/1800237420752912512.
[6] Cybersecurity and Infrastructure Sec. Agency, *Scattered Spider* (Nov. 16, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a.
[7] *Understanding Scattered Spider, and How They Perform Cloud-Centric Identity Attacks* (May 2, 2024), https://www.scmagazine.com/native/understanding-scattered-spider-and-how-they-perform-cloud-centric-identity-attacks.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

if it was paying any attention, that the electronic records and PII it maintained would be targeted by cybercriminals and ransomware attack groups.

51. Defendant knew or should have known that these attacks were common and foreseeable.

52. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

53. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

54. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

55. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to companies storing sensitive PII, like Defendant.[8]

56. Defendant knew and understood unprotected or exposed PII in the custody of

[8] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

insurance companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

57. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

D. Defendant Fails to Comply with FTC Guidelines.

58. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

59. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[9] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[10]

60. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the

[9] Federal Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[10] *Id*.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

network; and verify that third-party service providers have implemented reasonable security measures.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. These FTC enforcement actions include actions against private universities like Defendant.

63. Defendant failed to properly implement basic data security practices.

64. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers and other impacted individuals' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

65. Defendant was at all times fully aware of its obligation to protect the PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Fails to Comply with Industry Standards.

66. Several best practices have been identified that at a minimum should be implemented by companies storing sensitive PII like Defendant, including but not limited to educating all employees; requiring strong passwords; implementing multi-layer security, including firewalls, anti-virus and anti-malware software, centralized logging and monitoring systems; implementing encryption techniques, making data unreadable without a key; requiring and enforcing multi-factor authentication; backing up data; and limiting which employees can access sensitive data.

67. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

68. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

69. Defendant furthermore failed to have basic policies in place to require the foregoing safeguards and to prepare for the inevitable attack that did occur, including a sufficient incident response plan and a business continuity and disaster recovery plan that would have allowed Defendant to more seamlessly respond to the Data Breach in a way that would have allowed it to continue business operations, make payments to customers, quickly and efficiently remove the attacker from its information systems, and allow it to more fully understand the root cause of the Data Breach in a timely manner.

70. These foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

F. Defendant's Breach

71. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and website's application flow. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. failing to adequately protect PII;

c. failing to properly monitor their own data security systems for existing

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

intrusions;

d. failing to utilize centralized monitoring, alerting, and anomaly detection systems to identify malicious activity;

e. failing to implement appropriate system-level logging to ensure forensics artifacts would be maintained sufficient to identify the root cause of an attack and the full scope of what data was stolen or unauthorizedly accessed;

f. failing to ensure that their vendors with access to their computer systems and data employed reasonable security procedures;

g. failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;

h. failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;

i. failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

j. failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

k. failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;

l. failing to train all members of their workforces effectively on the policies and procedures regarding PII;

m. failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

n. failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTCA;

o. failing to adhere to industry standards for cybersecurity as discussed above;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

and,

p. otherwise breaching their duties and obligations to protect Plaintiffs' and Class Members' PII.

72. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access Defendant's computer systems, which provided unauthorized actors with unsecured and unencrypted PII.

73. Accordingly, as outlined below, Plaintiffs and Class Members now face a present, increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant, have suffered invasions of their privacy, and have suffered other financial harm, including the deprivation of the funds they were promised by Defendant.

G. Data Breaches Cause Disruption and Increased Risk of Fraud and Identity Theft.

74. Cyberattacks and data breaches at companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

75. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[11]

76. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

[11] *See* U.S. Gov. Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (2007), https://www.gao.gov/new.items/d07737.pdf.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

77. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

78. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

79. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

80. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[13]

81. Its value is axiomatic, considering the value of "big data" in corporate America and

[12] *See* Federal Trade Comm'n, https://www.identitytheft.gov/Steps.

[13] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

82. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII is stolen and when it is used.

83. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

84. PII is such a valuable commodity to identity-thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

85. PII can sell for as much as $363 per record according to the Infosec Institute.[15] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for many years.

86. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which

[14] *See* U.S. Gov. Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (2007), https://www.gao.gov/new.items/d07737.pdf.

[15] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.

87. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

88. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [16] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[17]

89. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[18]

90. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[19] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get

---

[16] *See* Social Sec. Admin., *Avoid Identity Theft: Protect Social Security Numbers*, SSA.GOV, https://www.ssa.gov/phila/ProtectingSSNs.htm (last visited Aug. 8, 2024).
[17] *Id.*
[18] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf.
[19] *See How to Protect Yourself from Social Security Number Identity Theft*, EQUIFAX, https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

medical treatment, and steal your government benefits."[20]

91. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

92. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[21]

93. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and

[20] *See* Julian Kagan, *What is an SSN? Facts to Know About Social Security Numbers* (Feb. 15, 2024), https://www.investopedia.com/terms/s/ssn.asp.

[21] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

target her in fraudulent schemes and identity theft attacks.")

94. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[22]

95. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[23]

96. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[24]

97. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[25]

---

[22] *See Your Social Security Number: Controlling the Key to Identity Theft*, AOG.CA.GOV, https://oag.ca.gov/idtheft/facts/your-ssn.

[23] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[24] *See* N.C. Gen. Stat. § 132-1.10(1).

[25] *See* Husayn Kassai, *Banks need to stop relying on Social Security numbers*, AMERICAN BANKER (Nov. 12, 2018), https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

98. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[26] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[27]

99. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[28]

100. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

101. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII

---

[26] *See* Ann Carrs, *Just 5 Banks Prohibit Use of Social Security Numbers*, NY TIMES, (Mar. 20, 2013), https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers.

[27] *See What Can Someone Do With Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597.

[28] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sept. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

102. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

103. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

104. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

105. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

106. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

107. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

108. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

109. Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

110. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of PII involved, there is a strong probability that entire batches of stolen information have

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

111. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her PII was used to file unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

112. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

113. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

H. Plaintiffs' and Class Members' Damages

114. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered because of the Data Breach.

115. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach, yet Plaintiffs have yet to receive a notification letter explaining what happened.

116. Upon information and belief, Plaintiffs and Class Members' PII, including full names and social security numbers, were compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's systems maintaining PII. This PII was acquired by unauthorized, unidentified third-party threat actors.

117. Since being notified of the Data Breach, Plaintiffs have spent significant time dealing with the impact of the Data Breach, valuable time that Plaintiffs otherwise would have spent on other activities, including but not limited to work and/or recreation.

118. Due to the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis trying to mitigate and address harms caused by the Data Breach. This includes

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

changing passwords, cancelling credit and debit cards, and monitoring their accounts for fraudulent activity.

119. Plaintiffs and Class Members have also suffered financial harm in the form of delayed, partial, or absent payments that Defendant owed them from the sale or trade-in of their vehicles.

120. Plaintiffs' PII was compromised as a direct and proximate result of the Data Breach.

121. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

122. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

123. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft because Defendant allowed all the ingredients of identity theft to fall into the hands of cybercriminals.

124. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

125. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

126. Plaintiffs and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

127. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and sensitive information for misuse.

128. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses. Plaintiffs' Class Members' valuable time they reasonably incurred to remedy or mitigate the effects of the Data Breach includes:

a. reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. purchasing credit monitoring and identity theft prevention;

c. placing "freezes" and "alerts" with reporting agencies;

d. spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. contacting financial institutions and closing or modifying financial accounts;

f. closely reviewing and monitoring Social Security numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come; and,

g. contacting Defendant's dealerships and attempting to be paid the money owed to them by Defendant because of agreements to sell or trade-in vehicles.

129. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in Defendant's possession, is protected from further breaches through the implementation of adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected, that Defendant has sufficient policies and training in place, that all of Defendant's systems are encrypted and protected by multi-factor authentication, and that Defendant's systems are appropriately patched with the latest security updates.

130. Further, because of Defendant's conduct and failures, Plaintiffs and Class Members are forced to live with the stress and anxiety that their PII may be disclosed to the entire world, or at least to even further cybercriminals, thereby subjecting them to embarrassment, further risk of

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

identity theft, and depriving them of the autonomy to decide who has access to the most sensitive and private information, including their financial information and identifying information that they cannot change.

131. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered economic harms, anxiety, stress, emotional distress, loss of privacy, and are at an increased risk of future harm.

I. Plaintiffs' Experiences

Plaintiff Smith

132. Plaintiff Karen Smith (for purposes of this section, "Plaintiff") provided her information to Defendant as a condition of purchasing a vehicle from Defendant in 2018.

133. Plaintiff provided her PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

134. Upon information and belief, Plaintiff's PII was compromised in the Data Breach.

135. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

136. Defendant has deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it in a timely manner.

137. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after learning of the Data Breach.

138. Plaintiff has spent significant time attempting to mitigate the impact of the Data Breach and will continue to spend valuable hours for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

139. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of his privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

increased risk of identity theft and fraud.

140. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

141. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

142. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Bouphapraseuth

143. Plaintiff Bouphapraseuth (for purposes of this section, "Plaintiff") provided his information to Defendant as a condition of purchasing a vehicle from Defendant in 2017.

144. Plaintiff provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

145. Upon information and belief, Plaintiff's PII was compromised in the Data Breach.

146. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

147. Defendant has deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it in a timely manner.

148. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after learning of the Data Breach.

149. Plaintiff has spent significant time attempting to mitigate the impact of the Data

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Breach and will continue to spend valuable hours for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

150. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of his privacy rights; (c) the theft of his PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

151. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

152. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his life.

153. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Farrell

154. Plaintiff Ryan Farrell (for purposes of this section, "Plaintiff") provided his information to Defendant as a condition of purchasing and doing business with Defendant.

155. A few weeks before Defendant's Data Breach, Plaintiff traded in a vehicle at one of Defendant's Honda dealerships.

156. As part of this transaction, Plaintiff was required to provide his PII to Defendant and trusted that Defendant would use reasonable and industry standard cybersecurity measures to protect his information according to Defendant's internal policies, as well as state and federal law,

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

and because Defendant is a major, sophisticated automobile dealership in the area.

157. Defendant agreed to purchase a vehicle from Plaintiff, accepted delivery of that vehicle, and then failed to fully compensate Plaintiff.

158. As part of the Parties' trade-in contract, Plaintiff purchased a new vehicle, applied have of the trade-in amount to the purchase price of the new vehicle, and then Defendant promised to remit payment for the remainder—$2,500—to Plaintiff.

159. Defendant failed to tender payment in a timely manner. Though the payment was eventually made, Plaintiff was deprived the use of the money owed for weeks because of Defendant's failures to properly prepare for an imminently foreseeable cyberattack.

160. When Plaintiff inquired as to why he had not been paid, Defendant's employees told him that Defendant's systems were shut down because of the Data Breach and that they were unable to process his payment.

161. Later, Defendant again promised to tender payment, but when that did not happen, Defendant told Plaintiff their print services were down. Then, Defendant said its finance system had been breached again and so Defendant was again unable to pay.

162. Upon information and belief, Plaintiff's PII was compromised in the Data Breach.

163. Plaintiff is very careful with his sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or through any other unsecured means.

164. Defendant has deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about regarding the details of the Data Breach, including how it occurred, what steps Defendant is taking to mitigate its affects, what steps Defendant is taking to prevent it from happening again, or even how Defendant is able to identify the scope of the Breach.

165. Defendant has failed to be transparent with the public, and so Plaintiff and Class Members are left in the dark regarding the Data Breach.

166. Because of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

of the Data Breach after learning of the Data Breach, especially given the recency of his transaction with Defendant, that it had not been completely, and thus that Defendant necessarily still had his private financial information.

167. Plaintiff has spent significant time attempting to mitigate the impact of the Data Breach and will continue to spend valuable hours for the remainder of his life that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

168. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of his privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

169. Plaintiff also suffered economic harm an amount not less than $2,500, interest on that principle, and the value of the time he has been deprived of his money assets.

170. As a result of the Data Breach, Plaintiff has also suffered emotional distress due to the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

171. Because of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

172. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Stevens

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

173. Plaintiff Stevens (for purposes of this section, "Plaintiff") provided her information to Defendant as a condition of purchasing a vehicle from Defendant in 2023.

174. Plaintiff provided her PII to Defendant and trusted that it would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

175. Upon information and belief, Plaintiff's PII was compromised in the Data Breach.

176. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

177. Defendant has deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it in a timely manner.

178. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach after learning of the Data Breach.

179. Plaintiff has spent significant time attempting to mitigate the impact of the Data Breach and will continue to spend valuable hours for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

180. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant maintained belonging to Plaintiff; (b) violation of her privacy rights; (c) the theft of her PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

181. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a result of the release of her PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

182. As a result of the Data Breach, Plaintiff anticipates spending considerable time and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of her life.

183. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Sax

184. Plaintiff Jay Sax (for purposes of this section, "Plaintiff") provided his information to Defendant as a condition of purchasing a car and doing business with Defendant.

185. Plaintiff recently purchased a vehicle from one of Defendant's Honda dealerships.

186. As part of that transaction, Defendant was responsible for registering the vehicle.

187. Plaintiff is an Uber driver and earns on average around $150 per day as an Uber driver.

188. In mid-June, after purchasing the vehicle from one of Defendant's dealerships, Plaintiff began receiving notifications from Uber that the car's registration needed to be updated.

189. Because Defendant was responsible for providing the registration documents, Plaintiff began calling Defendant to ask for a status update.

190. After Plaintiff tried calling dozens of times with no answer, one of Defendant's employees finally answered and informed Plaintiff that the delays were caused by Defendant's "internet problems."

191. Defendant's employees represented that they would send the registration information in a matter of minutes, but that did not happen.

192. Defendant's failures have caused Plaintiff to spend more than a dozen hours of his valuable time attempting to call Defendant to understand the delays, find out more information, and to attempt to get his car registered.

193. On December 27, more than three days after Plaintiff's temporary registration expired, preventing Plaintiff from being able to earn money as an Uber driver, Defendant finally

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

sent Plaintiff the Electronic Dealer Report of Sale ("EDRS") documentation so that Plaintiff could register the car himself.

194. Because of the Data Breach, Defendant's failure to have appropriate contingency plans in place, and Defendant's failure to appropriately safeguard against the foreseeable threat of a data breach, and because of the resulting system interruptions, Defendant has been unable to operate normally, its systems have largely been offline, and these failures have caused Plaintiff to lose money in the form of time spent attempting to deal with Defendant's failures and lost income from being unable to work as an Uber driver for days.

195. Moreover, Defendant's failures caused Plaintiff's sensitive PII to fall into the hands of cybercriminals. For example, Defendant collected Plaintiff's credit card information for the car purchase. Because Plaintiff's PII and financial information is now likely in the hands of cybercriminals bent on identity theft, Plaintiff has taken the steps recommended to him to review financial and credit accounts, contacting banks, and keep a vigilant eye out for fraudulent activity.

CLASS ACTION ALLEGATIONS

196. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class") pursuant to Nevada Rule of Civil Procedure 23.

197. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose PII was compromised in the Data Breach or have otherwise suffered harm because of the Data Breach (the "Class").

198. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families, and members of their staff.

199. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

200. The proposed Class meets the criteria for certification under Nevada Rules of Civil

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

Procedure 23(a) & (c).

201. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in the Data Breach.

202. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. if Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. if Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. if Defendant owed a duty to Class Members to safeguard their PII;

f. if Defendant breached their duty to Class Members to safeguard their PII;

g. if Defendant knew or should have known that their data security systems and monitoring processes were deficient;

h. if Defendant should have discovered the Data Breach sooner;

i. if Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. if Defendant's conduct was negligent;

k. if Defendant's breach implied contracts with Plaintiffs and Class Members;

l. if Defendant were unjustly enriched by unlawfully retaining a benefit

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

conferred upon them by Plaintiffs and Class Members;

m. if Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. if Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

203. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

204. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

205. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

206. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

207. Class certification is also appropriate under Nevada Rule of Civil Procedure 23(c)(2). Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

208. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
Negligence and Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

209. Plaintiffs repeat and re-allege the preceding paragraphs and incorporate them by reference herein.

210. Plaintiffs and the Class entrusted Defendant with their PII on the premise and with the understanding that Defendant would safeguard their information, use their PII for admissions purposes only, and/or not disclose their PII to unauthorized third parties.

211. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

212. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

213. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

214. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and individuals who entrusted them with PII, which is recognized by laws and regulations, as well as common law. Defendant was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach. Moreover, Defendant's duty arose out of Nevada statutory law, which requires Defendant to implement reasonable cybersecurity measures. Nev. Rev. Stat. § 603A.210(1).

215. Defendant's duty to use reasonable security measures required Defendant to reasonably protect confidential data from any intentional or unintentional use or disclosure.

216. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

217. The purpose of the FTC Act is to protect consumers from unfair and deceptive practices, like the failure to implement reasonable, industry standard cybersecurity safeguards, and to protect those consumers from the harms associated with data breaches.

218. Moreover, Defendant was required to implement reasonable cybersecurity measures under the Nevada Data Breach Notification statute. Nev. Rev. Stat. § 603A.210(1) ("A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure.").

219. The Nevada Data Breach Notification statute is particularly designed to protect consumers from the type of harms attendant to data breaches, including identity theft, fraud, and extortion. Thus, because Defendant violated the requirement, it was negligent per se.

220. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential PII.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

221. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. failing to adequately monitor the security of their networks and systems;

d. failing to have in place mitigation policies and procedures;

e. allowing unauthorized access to Class Members' PII;

f. failing to detect in a timely manner that Class Members' PII had been compromised; and

g. failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

222. Defendant owed to Plaintiffs and Class Members a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

223. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, among other requirements, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; (iii) implement written cybersecurity policies, including sufficient incident response, disaster recovery, and business continuity plans that include lessons learned from this Data Breach; and (iv) to continue to provide adequate credit monitoring to all Class Members.

224. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs'

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

and Class Members' PII.

225. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and Class Members' PII.

226. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

227. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it.

228. Defendant breached its duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and Class Members—which actually and proximately caused the Data Breach and injured Plaintiffs and Class Members.

229. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

230. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of an Express Contract
(On Behalf of Plaintiffs and the Class)

231. Plaintiffs repeat and re-allege the preceding paragraphs and incorporate them by reference herein.

232. Defendant enters into express agreements with its customers to perform the services and sell the vehicles those customers request.

233. These contracts include express agreements to perform that Defendant failed to uphold because of the Data Breach.

234. For example, trade in contracts require the consumer to provide Defendant with a vehicle when purchasing a new or pre-owned vehicle, and Defendant provides compensation to consumers some of which is paid directly to the consumer and some of which goes to the purchase of the vehicle.

235. Contracts for maintenance on vehicles include the expectation that the vehicle will be returned in a timely manner. And vehicle purchases include the contractual requirement that Defendant register vehicles in a timely manner so that customers can continue to use those vehicles once the temporary period ended.

236. Because of the cyberattack on Defendant's systems, it was unable to perform under these contracts, causing harm to Plaintiffs and the proposed Class Members.

237. Indeed, on at least one occasion, when Plaintiff Farrell asked about the money owed, he was told the delay was because Defendant was unable to process checks because of the cyberattack.

238. Because of Defendant's breach of contract, Plaintiffs have been deprived of the benefits of the contract, for which they are entitled to damages.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

239. Plaintiffs repeat and re-allege the preceding paragraphs and incorporate them by reference herein.

240. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of leasing or purchasing a vehicle from Defendant or as a condition of receiving maintenance on their vehicles. Plaintiffs and Class Members provided their PII to Defendant or its third-party agents in exchange for Defendant's services and/or products.

241. Plaintiffs and Class Members reasonably understood that a portion of the funds they paid Defendant for their vehicles would be used to pay for adequate cybersecurity measures.

242. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that it was required to provide based on Defendant's duties under state and federal law and its internal policies.

243. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for services and/or employment.

244. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

245. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

246. After all, Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

247. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

248. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

249. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

250. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

251. In these and other ways, Defendant violated its duty of good faith and fair dealing.

252. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

253. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

254. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT IV
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

255. repeat and re-allege the preceding paragraphs and incorporate them by reference herein.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

256. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

257. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

258. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

259. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

260. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

261. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

262. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant was on notice that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

263. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

264. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

265. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

266. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

267. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

268. Plaintiffs repeat and re-allege the preceding paragraphs and incorporate them by reference herein.

269. This count is pleaded in the alternative to breach of contract claims.

270. Plaintiffs and Class Members conferred a benefit, including their valuable PII, on Defendant in connection with their purchase or lease of vehicles from Defendant. In so conferring this benefit, Plaintiffs and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

271. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

272. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

273. Under the principle of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members,

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

274. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

275. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

276. Plaintiffs and Class Members have no adequate remedy at law.

277. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures as long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the impact of the PII comprised as a result of the Data Breach for the reminder of the lives of Plaintiffs and Class Members.

278. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

279. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

COUNT VI
Declaratory Judgment and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

280. Plaintiffs repeat and re-allege the preceding paragraphs and incorporate them by reference herein.

281. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

282. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

283. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII it possesses, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTCA and under Nevada law Nev. Rev. Stat. § 603A.210(1);

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and

c. Defendant's breach continues to cause harm to Plaintiffs and the Class.

284. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its prospective, current and/or former consumers' (i.e., Plaintiffs' and the Class') data.

285. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

286. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

287. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order;

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiffs' and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats,

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: August 16, 2024

Respectfully Submitted,

By: */s/ Nathan R. Ring*

Nathan R. Ring
Nevada Bar No.12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Tel: (725) 235-9750
lasvegas@stranchlaw.com

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

Grayson Wells (TN 039658)*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gwells@stranchlaw.com

Steven Sukert (FBN 1022912)+
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: 954-525-4100
sukert@kolawyers.com

John J. Nelson (SBN 317598)*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Tel: (858) 209-6941
jnelson@milberg.com

**Pro Hac Vice Application Forthcoming*
+ Pro Hac Vice Application Submitted
Counsel for Plaintiffs and the Proposed Class

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on August 16, 2024, the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Suzanne Levenson
Suzanne Levenson

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC